ダウンロード・データあります　ご購入はこちら

パケットづくりではじめるネットワーク入門

第21回　さすが次世代PcapNG…パケットにコメント等の付加情報を追加する

坂井 弘亮

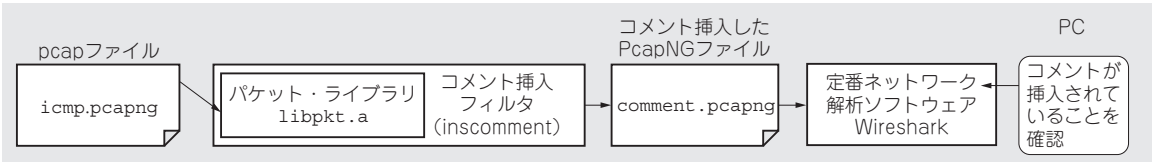

図1　今回すること…次世代PcapNGパケットのオプション領域にコメント（付加情報）を挿入できるようにする
コメント挿入したPcapNGファイルを定番解析ソフトウェアWiresharkで確認してみる

本連載はネットワーク上を流れるパケットを直接扱うようなツールを自作しつつ，ネットワークの仕組みを勉強していきます．テーマは「自作」，「現物ベース」，「動く感動」の3つです．ネットワークにはイーサネットとIPを想定しています．

● 今回すること…次世代PcapNGのオプション領域にコメント等の付加情報を追加する

前回までは，ネットワーク・パケットを保存するための次世代フォーマットであるPcapNGフォーマットの入出力方法について説明し，pcapフォーマットをPcapNGフォーマットに変換するコンバータや，その逆を行う逆コンバータを作成しました．

今回はPcapNGのオプション領域（**図1**）を利用してコメントなどの付加情報を追加する方法について説明し，パケットにコメントを入れるコメント挿入フィルタを作成します．

次世代PcapNGに付加情報を追加できるオプション領域

● 特徴…コメントやツール独自の情報などを格納できる

PcapNGは各ブロックにオプション領域を持つことができます．

例えば**図2**はパケットを格納するためのEPB（Enhanced Packet Block）のフォーマットです（第19回，2017年2月号説明）．

パケット・データの後（ブロックの末尾）にはオプション領域を持つことができます．これは通常は付加されていないのですが，オプション機能としてコメントやツール独自の情報などを格納できます．

● 構造

PcapNGの仕様は，以下に記載されています．

`http://pcapng.com/`

上記サイトの「Pcap-NG specification」がPcapNGの仕様です．オプション領域の仕様は2.5章に説明があります．その仕様は**図3**のようになっています．

先頭2バイトのオプション・コードによってオプションの種別を判断します．オプション・コードはコメントの場合は「1」です．

また後続の2バイトにオプション値のバイト・サイズが格納されています．これはオプション・コードや

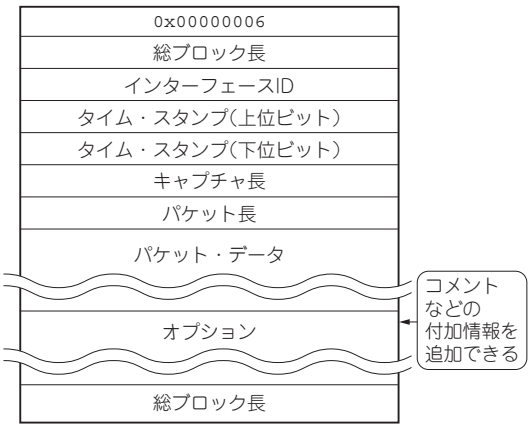

図2　次世代フォーマットPcapNGでパケット・データを格納するEPBには付加情報を追加できる

本連載のプログラムのソースコードは以下の筆者のホームページからダウンロードすることができます．ライセンスはKL-01というもので，組込み機器などでも自由に利用することができます．
`http://kozos.jp/books/interface/ethernet2/`